HUNTON
ANDREWS KURTH

May 9, 2022

Vanessa A. Countryman
Secretary
Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-1090

Via email: rule-comments@sec.gov

Re: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure
File No. S7-09-22

Dear Ms. Countryman:

We are submitting this letter in response to the solicitation by the Securities and Exchange Commission (the "Commission") for comments on the Commission's proposed rules (the "Proposed Rules") regarding Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure. The Proposed Rules were set forth in Release Nos. 33–11038; 34–94382; IC–34529, published in the Federal Register on March 23, 2022 (the "Proposing Release").[1]

More than twenty years ago, Hunton Andrews Kurth LLP was among the first law firms to establish a dedicated privacy and cybersecurity practice. We regularly work with clients to address a broad range of issues related to cybersecurity, and have been called upon to assist with every phase of data breach management, from preparedness and prevention to mitigation and resolution. We have extensive experience working on cybersecurity matters before the Commission, the Federal Trade Commission, other state and federal law enforcement authorities, state attorneys general, EU data protection authorities, and numerous other foreign government regulators. We have managed more than 2,000 data breaches and cybersecurity events worldwide, and are regularly called upon to provide counsel on highly complex, large-scale cybersecurity incidents. Of particular relevance to the Proposed Rules, these engagements frequently require us to advise publicly-traded companies and other SEC registrants on their corporate governance and SEC disclosure obligations associated with cybersecurity matters.

We respectfully request that the Commission consider the following recommendations for changes and clarifications to the Proposed Rules were they ultimately to be adopted as final rules (as so adopted, "Final Rules"). In providing these comments, we express no view

[1] 87 Fed. Reg. 16,590 (Mar. 23, 2022).

as to the Commission's authority to adopt Final Rules or the administrative rulemaking process more generally.

1. The Commission should refine the definition of "cybersecurity incident."

The Proposed Rules would define a "cybersecurity incident" as "an unauthorized occurrence on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein." Our principal concern is with the use of the verb "jeopardizes," which is a critical element of the overall definition. We believe the term is too imprecise for a Final Rule and should instead be replaced with terminology more clearly indicating actual adverse effect.

While the word "jeopardize" is used in other cybersecurity regimes and is incorporated into the definition of cyber incident in the recently-enacted Cyber Incident Reporting for Critical Infrastructure Act, it is not one that appears regularly (if at all) in the Commission's existing regulations or disclosure forms. "Jeopardize" seems more tenuous and speculative than the *Basic v. Levinson* materiality test for forward-looking statements that calls for a balancing of the "indicated probability" of an event and its "anticipated magnitude".[2] In the Proposing Release, the Commission seems to confirm the hypothetical nature of the term by stating, "We believe this term is sufficiently understood and broad enough to encompass incidents that *could* adversely affect a registrant's information systems or information residing therein" (emphasis added).[3]

Because "jeopardize" is not a term of art to securities practitioners, there is no well-accepted understanding of the breadth of the verb in the context of disclosure under the federal securities laws. Lacking a common understanding, we believe the subjectivity and ambiguity of the term "jeopardize" will lead to countless interpretive difficulties whenever disclosure may be required. The use of a materiality qualifier would not by itself, in our view, help to resolve these challenges.

Further, use of the term "jeopardize" may require disclosure of inchoate effects when no actual harm has occurred. Placing something in jeopardy implies creation of the risk of loss or risk of damage, but it does not necessarily follow that actual harm will in fact occur. Item 105 of Regulation S-K already provides a thorough treatment of when risk factor disclosure is required in periodic reports and registration statements, and Item 303 already requires disclosure about material uncertainties that is well understood. Generally accepted

[2] *Basic v. Levinson*, 485 US 224, 238-9 (1988).
[3] Proposing Release, 87 Fed. Reg. at 16,596 n. 58.

accounting principles require disclosure of loss contingencies. We do not believe the definition here should lead to the disclosure of events that may cause risk but no actual harm.

Accordingly, we do not see a compelling need to create a duplicative disclosure requirement for cybersecurity. Moreover, in the case of disclosure on Form 8-K, the disclosure of a speculative, forward-looking event would be inconsistent with the other disclosure items on the form, which uniformly call for the disclosure of historical information that is certain and complete.

As alluded to above, we instead recommend that the Commission key a cybersecurity incident off occurrences associated with actual adverse impacts. As such, the revised definition in any Final Rule would read "an unauthorized occurrence on or conducted through a registrant's information systems that ~~jeopardizes~~ **adversely effects** the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein." In this way, the revised definition clarifies that only those unauthorized occurrences that cause harm are the subject of the definition, not merely those occurrences that have the potential to do so. This revision also more closely aligns the definition with the proposed definition of "cybersecurity threat," which likewise keys off the concept of adverse effects.

2. The four business-day deadline under the proposed revision to Form 8-K is too short.

As currently drafted, Proposed Item 1.05 of Form 8-K would require disclosure within four business days of when a registrant determines that a cybersecurity incident is material. A proposed instruction to this item would require a registrant to make the materiality determination "as soon as reasonably practicable after discovery of the incident." We believe a rapid materiality determination should not be the trigger for disclosure, and instead disclosure should be required no sooner than 30 days after the materiality determination.[4]

Even before any materiality determination is or could be made, the initial days after discovery of any significant cyber event are often highly tense and a great sense of uncertainty proliferates. Many companies conduct simulations and tabletop exercises in advance to gain a greater sense of preparation, and written cybersecurity incident response plans are becoming more common, but are by no means universal. Even the best-prepared companies encounter challenges and difficulties in marshaling a response to an actual incident, with the challenges and difficulties multiplying as the scale of the incident increases.

[4] Although our comments in this section are primarily directed at the proposed disclosure requirement under Form 8-K, we believe foreign private issuers also face similar challenges under the Commission's proposed Form 6-K requirement.

In response, forensic cybersecurity investigators and other outside professionals (including counsel) must be quickly retained. Evidence must be preserved. Breach notification laws must be reviewed and, when applicable, complied with. Identifying the scope of the breach or other incident is often complicated and time-consuming, and can take weeks or months to complete. Remedial efforts must begin. Law enforcement must be notified. Insurance claims must be made. When critical operations or infrastructure are impacted, contingency plans must be set in motion to mitigate further business interruption. The presence of ransomware may compel the registrant to open negotiations with the threat actor, which itself is a highly complex issue. These and other critical response steps very much transpire in a "fog of war" atmosphere. These challenges are magnified when a registrant's vendor or another third party is the ultimate target of the breach.

Under these circumstances, adding an additional immediate disclosure obligation is likely to further complicate a registrant's response to the incident. Pressure to make disclosure rapidly, before key facts are known and adverse impacts on the business understood, is likely to lead to disclosure that is incomplete or incorrect. In our view, investors do not benefit from imperfect disclosure that must be corrected or then amended subsequently. Further, efforts to contain and remediate the incident or provide assistance to law enforcement could be compromised by premature public disclosure in the detail the Proposed Rules require. In a worst case scenario, premature disclosure could exacerbate an already tense situation.

Rather than compel a hasty disclosure before key facts are understood and impacts appreciated, we believe using a 30-day deadline as the disclosure trigger would mitigate these concerns.[5] While state data breach notification laws vary from state to state, 30 days from the cybersecurity incident is the earliest date any state requires that notification to affected persons be made. These state laws recognize and accommodate the practical difficulties of making widespread disclosure in a short period of time. Synchronizing the SEC deadline with state data breach notification standards ensures that the SEC reporting deadline does not precede the first notifications due to individuals or entities whose data may be implicated in the cybersecurity incident.

At the point in time when a cyber incident is remediated, registrants will generally have a much clearer picture of the details surrounding it, such as whether any data was stolen or used for an unauthorized purpose, as well as the effect of the incident on the registrant's operations—all items called for under the proposed Form 8-K disclosure. Disclosure made at

[5] States with a 30-day deadline include Florida (Fla. Stat. § 501.171(4)(a)) and Maine (10 Me. Rev. Stat. §1348). Other states such as Alabama have a 45-day deadline (Ala. Stat. §8-38-5), and Connecticut has a 60-day deadline, which was recently shortened from 90 days (Conn. Gen. Stat. § 36a-701b(b)).

this point in time is also less likely to require future revision, and is more likely to provide investors with actionable information to aid them in making future investment decisions.

3. The Commission should not require aggregation of immaterial events for purposes of determining whether a cybersecurity incident has occurred.

Proposed Item 106(d)(2) of Regulation S-K would require disclosure when a series of previously undisclosed individually immaterial cybersecurity incidents become material in the aggregate. The Proposing Release notes that such incidents could take a variety of forms, and provides the single example where one malicious actor engages in a number of smaller but continuous cyber-attacks related in time and form against the same company and collectively, they are either quantitatively or qualitatively material, or both. We do not believe the Commission should require aggregation of immaterial events for purposes of determining whether a cybersecurity incident has occurred.

First, we do not believe disclosure of this information would be decision-useful to investors. In our experience, many businesses experience dozens (and sometimes hundreds) of immaterial events on a daily or weekly basis that, when aggregated, may require disclosure under proposed Item 106(d)(2).[6] The situation is particularly acute in financial services, for critical infrastructure providers, and for consumer-facing industries such as retail and healthcare, but the situation is not unique to them. The volume and frequency of these events, if required to be disclosed in SEC periodic reports, would instead lead to the "avalanche of trivial information" that is "hardly conducive to informed decisionmaking"[7] as the Supreme Court has cautioned against.

Beyond the single example cited in the Proposing Release, the Proposed Rules provide little additional guidance as to when a series of otherwise seemingly unrelated events should be aggregated. The lack of guidance is surprising since this requirement could easily lead to the largest volume of new disclosure under the Proposed Rules. In most other disclosure contexts under the federal securities laws, the practice of bundling otherwise unrelated, immaterial events for reporting purposes would be unusual and is not generally required. Further, the techniques threat actors deploy are constantly evolving, as are the techniques they use to conceal their true identities. It is not always readily apparent, for example, that a single threat actor is behind a series of otherwise seemingly unrelated events, such as a series of impersonation attacks or a series of credential-stuffing attacks.

---

[6] The vast majority of these attempts are repelled through cybersecurity countermeasures, but could still be deemed to "jeopardize" the confidentiality or integrity of data.

[7] *TSC Industries, Inc. v. Northway, Inc*., 426 US 438, 448-9 (1976).

Even if the threat actor could be definitively identified, would disclosure be required if it conducted two immaterial attacks six months apart? Six years apart? Would registrants be required to aggregate similar immaterial events occurring over the same time span even if they were demonstrably initiated by different threat actors? These kinds of thorny interpretive questions are likely to become commonplace under proposed Item 106(d)(2), and are also likely to overwhelm both registrants and the Commission's Staff who would routinely be asked to provide interpretive advice.[8]

Finally, tracking the data necessary to inform the disclosure decision would pose significant technical compliance challenges to many registrants, particularly smaller reporting companies and emerging growth companies. While more sophisticated information security functions keep daily event logs and use both manual analysis and artificial intelligence techniques to search for patterns and anomalies, use of these methods is often expensive, time-consuming and not uniformly practiced. Even among sophisticated businesses there is much variability in the processes and the outcomes. Further, without detailed guidance from the Commission as to exactly the kinds of situations that would require aggregation, it would be exceedingly difficult for software engineers to design algorithms to identify the kinds of still-unclear fact patterns the Commission hopes to capture. Again, smaller reporting companies and emerging growth companies are particularly at a disadvantage in this respect.

4. The Commission should not require disclosure around a board cybersecurity expert.

Under proposed Item 407(j) of Regulation S-K, a registrant would be required to disclose if "any member of the board has cybersecurity expertise, . . . the names(s) of any such director(s) and provide such detail as necessary to fully describe the nature of the expertise." We urge the Commission to eliminate this disclosure requirement in any Final Rules.

Many boards currently lack a dedicated cybersecurity expert, and with good reason—the ability of the board of directors to provide oversight and monitor compliance in a manner consistent with its fiduciary duties is not dependent on having technical subject matter expertise. Boards instead rely on management and outside consultants to develop appropriate cybersecurity policies and procedures, as they are permitted to do under state law. The

[8] We see similarities to this kind of fact pattern and others where the Commission's Staff has made a policy decision not to provide any interpretive advice due to the potential volume of requests, the fact-intensive nature of the information, resource constraints, and other policy concerns. Examples of these situations in the Division of Corporation Finance include determinations of affiliate status and whether an issuer has perfected a private placement exemption in connection with a non-public offering of securities. Any absence of further guidance would compound the problem.

Commission oversees disclosure by registrants in countless regulated industries, and does not require each board to make disclosure about the technical or regulatory expertise of board members on an industry by industry or discipline by discipline basis, with the critical exception of the audit committee financial expert, which is a requirement derived from a congressional mandate under the Sarbanes-Oxley Act.

With the existing requirement of an audit committee financial expert, alongside the proposed requirement for a board climate expert under a parallel Commission rulemaking,[9] there exists the potential for at least three separate board experts under Commission rules. Given the vastly different skill sets required for these three compliance specialties, we suspect relative few directors would be able to fill all three positions single-handedly. Further, reserving three compliance-oriented board seats would continue to tilt the balance away from strategic-focused boards and more towards compliance-focused ones, which is not a trend we believe is in the best interest of investors.

While risk management and legal compliance are certainly important functions for any board of directors, we do not believe specific cybersecurity expertise is required to discharge those responsibilities. Additionally, we believe management and compliance specialists are better suited to tackling tactical issues involving the specific details of mitigating a given risk factor, including cybersecurity. For some companies, cybersecurity risk is not material to the business, and in those circumstances we question the need to have a designated cybersecurity expert on the board.

Naming cybersecurity experts could also have the unintended consequence of placing them personally at risk to malicious action on the part of threat actors. Certain nation states may place named experts under official surveillance or otherwise harass or persecute them without due process. Hacktivists may try to embarrass the named directors by publishing their personal data or taking unauthorized control of personal computing devices in an effort to discredit a given director's cybersecurity acumen. Named directors may also be placed at other virtual or physical risks, and the prospect of such risk counterproductively may serve as a disincentive to board service in the first place.

Moreover, we believe there is a scarcity in the marketplace for technical experts who would satisfy the Commission's proposed criteria for a cybersecurity expert. We believe the proposed criteria to demonstrate cybersecurity expertise are unduly narrow, but we fear that even loosening the criteria substantially would do little to alleviate this shortage of human

[9] Release No. 33-11042, The Enhancement and Standardization of Climate-Related Disclosures for Investors, 87 Fed. Reg. 21,334 (Apr. 11, 2022).

capital. Those that satisfy whatever technical qualifications the Commission settles on may not satisfy the other wholistic criteria that boards consider when recruiting new directors.

The demands on chief information security officers and cybersecurity forensic investigators, two groups who would most likely satisfy any expert criteria the Commission conceives, may leave them with precious little free time to serve on another company's board of directors. Thus, as a practical matter, we believe the population of eligible candidates is too small to ensure that every reporting company has a board cybersecurity expert. Smaller reporting companies and emerging growth companies may struggle to recruit from the limited pool of candidates as those qualified to serve choose the boards of larger or better known companies. While proposed Item 407(j) is crafted so as to not mandate a board cybersecurity expert, we believe most registrants would be hesitant to disclose the absence of one if affirmative disclosure of that fact is required.

5. The Commission should provide for a law enforcement exemption to disclosure.

We believe there are many compelling circumstances when potential or ongoing civil or criminal investigations may necessitate a delay in reporting a cybersecurity incident to investors, particularly when national security concerns are implicated. We are therefore concerned that that the Proposed Rules make no allowance for a delay necessitated by law enforcement or national security concerns. In our experience, law enforcement agencies frequently encourage registrants to limit public disclosure pending resolution of a civil or criminal investigation. Premature disclosure of a cybersecurity event may also stress national security or foreign intelligence concerns. Although the needs of investors are certainly important, we do not believe the balance of equities tips in favor of investor disclosure when broader national security issues are at stake.

The solution that the Commission sought comment on but did not officially propose—a delay when the Attorney General issues a written determination it is in the interest of national security—is not likely to be workable in practice. We do not believe the Attorney General (or subordinates acting on his or her behalf) would be inclined to provide such a written determination for any number of reasons, such as those involving the confidentiality of the law enforcement process and other law enforcement priorities that may be impaired by written disclosure. As the Proposing Release notes, many state data breach laws provide for a law enforcement exemption, but in our experience the relevant state and federal law enforcement agencies seldom (if ever) provide written instructions when the relevant exception comes into play. Even if the Attorney General were motivated to provide a written instruction (a proposition for which we express substantial doubt), we do not believe the Attorney General would opine on matters outside the Department of Justice's jurisdiction, which would include many issues impacting national security that are under the ambit of other

federal agencies, such as the Department of Homeland Security, Department of State and the Department of Defense. In addition, we do not believe obtaining written assurances would be possible as a practical matter within the four business-day reporting window currently proposed for Form 8-K disclosure. Accordingly, a broader exception is necessary.

We do not believe the burden of establishing an exemption from disclosure should fall entirely on individual registrants. On matters truly impacting law enforcement or national security concerns, the Government—not private entities—is best suited to make these nuanced determinations, particularly when the threat actor is a nation state or international criminal syndicate. Ideally, a system of communication among state and federal regulators, including the Commission, would develop such that knowledge by one agency would be imputed to other relevant ones, or one agency would take the lead in notifying the others. Absent a clear congressional mandate to do so, however, we are not optimistic that such a system will develop organically any time soon. Further, we believe that with most data breaches (and particularly those implicating personal information, national security or other sensitive topics), a smaller knowledge group is often preferable to a larger one in the early days of the incident.

As an alternative to a Government-led notification system, the Commission could develop a confidential reporting system for breach information. Under this approach, a confidential Form 8-K would be filed with the Commission within the prescribed deadline to serve as notice of the cybersecurity incident to the Commission. Doing so would permit the Commission to use the information to further its statutory mission. Such a filing would be subject to confidential treatment automatically, would not immediately appear in the public-facing Edgar database, and would be deemed exempt from disclosure under the Freedom of Information Act under the exclusions relevant to law enforcement.

At such time as the relevant law enforcement agencies no longer object to public disclosure, the registrant would notify the Commission so that the confidential Form 8-K may be made publicly available in Edgar, in much the same way that confidential draft registration statements become part of the public record within a specified period before other events may occur, such as in that context launching a road show or the date of anticipated effectiveness. To ensure investors are not subordinated to other stakeholders, the proposed confidential filing exemption would not be available if the registrant makes public disclosure through another channel, such as voluntarily through a press release or by another widely-dissemination public communication.

* * * * *

We appreciate the opportunity to participate in this process and would be pleased to discuss our comments or any questions the Commission or the Staff may have. You may contact Lisa Sotto, Steven Haas and Scott Kimpel of this firm.

Sincerely,

HUNTON ANDREWS KURTH LLP